Statement for the Record
Gregory Garcia
Assistant Secretary for Cybersecurity and Communications
National Cyber Security Division
U.S. Department of Homeland Security

Before the
United States House of Representatives
Committee on Homeland Security
Subcommittee on
Emerging Threats, Cybersecurity and Science and Technology
October 17, 2007

Chairman Langevin, Ranking Member McCaul, and Members of the Subcommittee, I appreciate the opportunity to speak about the role the Department of Homeland Security (DHS) plays in securing control systems, including the tools and resources we have made available to owners and operators of control systems, our efforts to collaborate and share information with both the public and private sectors, and analysis of control system vulnerabilities to strengthen the Nation's control system security posture. These efforts support one of the Department's primary missions of advancing preparedness. As October is National Cyber Security Awareness Month, I think it is particularly appropriate to highlight the importance of control systems security and to discuss our efforts to date to raise awareness of the challenges and solutions to securing these important systems. I would also like to recognize Chairman Langevin's and Ranking Member McCaul's leadership in promoting National Cyber Security Awareness Month's goals, objectives, and activities among their colleagues and constituents through their Dear Colleague letter and co-sponsorship of the Congressional Resolution. Raising awareness about protecting our critical infrastructures among home users, academic institutions, and businesses, including our control systems owners and operators, is fundamental to improving our preparedness posture.

As the Assistant Secretary for Cybersecurity and Communications within DHS' National Protection and Programs Directorate (NPPD), I oversee our mission to prepare for and respond to incidents that could degrade or overwhelm the operation of our Nation's information technology (IT) and communications infrastructure. This responsibility includes the goal of ensuring the security, integrity, reliability, and availability of our IT and communications networks. Reducing risk to that portion of the 17 sectors designated as critical infrastructures is among Secretary Chertoff's highest priorities, and I am pleased to share with you the Department's ongoing efforts to address this priority.

"Control system" is a general term that encompasses several types of systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures. Control systems typically are remotely controlled devices used to operate physical processes in industries such as electricity, water, oil and gas, chemical, transportation, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (e.g., automotive, aerospace, and durable goods). These control systems are critical to the safe and secure operation of our highly interconnected and mutually dependent critical infrastructures. A successful cyber attack on a control system could potentially result in physical damage, loss of service, and/or economic impact.

Ensuring the security of these systems is essential, and that responsibility lies heavily with the private sector, which owns and operates over 85 percent of the Nation's critical infrastructures. DHS works closely with private sector owners and operators to provide expertise, analytical products, and education and training materials that help control systems stakeholders identify and reduce direct risks for control systems. DHS communicates and collaborates with many diverse organizations, including government agencies, industry associations, national laboratories, equipment vendors, and asset owners and operators to identify improvements and drive their adoption across the infrastructure community. Through its involvement in the community and public-private partnerships, DHS is able to successfully engage with private sector owners and operators on significant control systems cyber security challenges and enable their voluntary cooperation and participation in implementing improvements to enhance the overall preparedness and resilience of the Nation's critical infrastructure.

DHS has three main objectives for reducing cyber risk and securing control systems: provide guidance, develop and enhance partnerships, and prepare for and respond to incidents. DHS also leverages the expertise and activities of operational programs and strategic initiatives from across the Department and the U.S. Government and integrates these activities to reduce risk, respond to incidents, and foster a culture of preparedness within the control systems community.

DHS utilization of several information sharing mechanisms allows the Department to manage effectively the collection and dissemination of sensitive vulnerability information, which ultimately enables us to raise awareness of vulnerabilities and risk management efforts among the control systems community, influence security practices to reduce risk, and raise the security bar across all the critical infrastructure sectors.

First, DHS **provides guidance** to the control systems community through several mechanisms and activities, including risk reduction products, such as security implementation guidelines and recommended practices; outreach and awareness through education and training; and technology assessments to identify vulnerabilities.

One of our recent accomplishments with regard to risk reduction products is the development and implementation of the Control Systems Cyber Security Self Assessment Tool (CS^{2}SAT), which employs a systematic and repeatable approach that allows owners and operators to assess the cyber security posture of their control systems. Through the CS^{2}SAT, users input facility-specific control system information. The tool then provides users with a picture of their control systems architecture and an assessment of their cyber security posture. It also makes recommendations for improvements. The recommendations are derived from industry cyber security standards and are linked to a set of specific actions that can be applied to mitigate the identified security vulnerabilities. The Instrumentation, Systems and Automation Society (ISA), one of the largest global organizations for control systems, announced on October 4, 2007 that it will make the CS^{2}SAT available to their membership, which consists of over 30,000 automation professionals.

Another risk-reduction tool DHS sponsors for the control systems community is the Multi-State Information Sharing and Analysis Center (MS-ISAC) SCADA Procurement Project. We have worked closely with the MS-ISAC, the SANS Institute, the Department of Energy (DOE) Idaho National Laboratory, and representatives from government and industry to develop common procurement language that owners and regulators can incorporate into contracting mechanisms to ensure the control systems they are buying or maintaining have the best available security. The long term goal is to raise the level of control systems security through the application of robust procurement requirements. The Procurement Project has received very positive feedback from users, and the document has averaged more than 450 downloads per month from the MS-ISAC website where it was posted in January 2007.

DHS also provides education and training for our industry and government partners. Through our control systems security training courses, we have provided training to nearly 7,000 IT and control systems professionals on a range of topics, such as identifying control systems vulnerabilities, conducting risk assessments, and applying standards-based mitigation measures to improve security. We offer both classroom and web-based instruction modules and will be launching a new operations security course later this month. The web-based training has been especially popular with our partners with geographically dispersed systems and personnel.

In addition, in coordination with academia we developed a graduate school curriculum for Masters of Business Administration and Masters of Public Policy programs to aid faculty in developing courses on the security of critical infrastructures with an emphasis on control systems security. The curriculum provides materials on public policy, technical issues, and managerial principles associated with critical infrastructure resiliency. To date, the curriculum has been distributed to more than 100 faculty members at universities and related institutions.

DHS is working with the National Institute of Standards and Technology (NIST) to strengthen Federal standards and guidance regarding control systems security. Over the past year, NIST has been developing cyber security guidance and a compliance framework specifically tailored to control systems. The guidance component, Special Publication (SP) 800-82 (2nd draft), “Guide to Industrial Control Systems (ICS) Security,” provides an overview of control systems, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks. The compliance component, Special Publication (SP) 800-53, “Recommended Security Controls for Federal Information Systems,” defines the minimum security controls for Federal systems and was originally published in 2005 by NIST in accordance with the requirements outlined in the Federal Information Security Management Act (FISMA). We have worked closely with NIST to develop SP 800-82, and to ensure that control systems security was incorporated into the updated revised SP 800-53. These NIST standards together will provide important baseline security guidance for adoption by Federal owners and operators of control systems.

We are also working with NIST and several of the DOE National Laboratories to develop a catalog of control system security standards. This comprehensive catalog represents a compilation of practices inventoried from across the industry standards bodies and provides recommendations for enhancements to standards to increase the security of control systems from both cyber and physical attacks. While many of today’s standards appropriately address security factors, detailed guidance is needed to ensure adequate protection from cyber attacks on control systems. This catalog is specifically designed to provide a framework for developing or enhancing technical aspects of security standards. When completed, the catalog will serve as a foundational document available for any industry using control systems to develop and implement cyber security standards specific to their individual operating requirements.

Second, we are **developing and enhancing dynamic, cooperative relationships** with government, industry, academia, and our international counterparts to promote control systems security and leverage existing initiatives being conducted by government and industry. For example, DHS partners with other agencies to support research and development of secure technologies for control systems. Public-private partnerships are essential in our efforts to improve the security of control systems because, as noted previously, the private sector owns and operates most critical infrastructure.

The National Infrastructure Protection Plan (NIPP) framework and supporting Sector-Specific Plans (SSPs) provide a coordinated approach to critical infrastructure protection roles and responsibilities for Federal, State, local, tribal, international, and industry security partners. Utilizing the NIPP framework, DHS directed recent activity to validate and mitigate a control systems vulnerability affecting a number of critical infrastructure sectors. Numerous Federal agency partners worked closely with industry technical experts to assess the vulnerability and to develop sector-specific mitigation plans. We are pleased with the results of this partnership: it produced jointly developed mitigation guidance and allowed owners and operators within the affected sectors to take deliberate and decisive actions to reduce significantly the risk associated with this vulnerability.

Recognizing the importance of engagement with industry, DHS sponsors a number of groups to foster close collaboration and information sharing among the control systems community. The Process Control Systems Forum (PCSF) was established to accelerate the design, development, and deployment of more secure control systems. The PCSF includes a variety of stakeholders including both national and international representatives from government, academia, owners and operators, systems integrators, and vendors.

The Control Systems Cyber Security Vendors' Forum, a subgroup under the PCSF, facilitates communication in a trusted environment between industrial automation and equipment suppliers and control system service providers. The Vendors' Forum consists of 50 members from 27 domestic and international companies comprising 90 percent of the market share providing service to all 17 critical infrastructure sectors.

An example of this collaboration occurred earlier this year when members of the Vendors' Forum worked together to address the potential effects on control systems caused by the date change in the Daylight Saving Time (DST) standard. The change in DST impacted control systems in over 19 countries. The control systems community recognized the importance of this issue and worked with the DHS National Cyber Security Division's United States Computer Emergency Readiness Team (US-CERT) to develop a Technical Information Paper, "Daylight Saving Time Changes for 2007." The paper provided guidance to industry on mitigation measures and has been downloaded from the US-CERT website more than 500 times between April and July 2007.

Third, to **prepare for and respond to incidents**, DHS is improving situational awareness, analyzing vulnerabilities, and sharing information. Owners and operators can report general cyber incidents and vulnerabilities, including those related to control systems, to the US-CERT. Control systems technical experts are integrated into the US-CERT operations center to provide timely situational awareness information and assist with incident management.

DHS has developed processes for sharing sensitive information related to control systems vulnerabilities with Federal, State, and local governments, and control systems owners, operators, and vendors to improve control systems security within and across all critical infrastructure sectors. This process addresses the information flow from vulnerability discovery, to validation, public and private coordination, and outreach and awareness, as well as identifies the deliverables and outcomes expected at each step in the process. Information sharing between the government and the private sector is essential to this process, and it allows both sectors to identify gaps in preparedness capabilities among public and private sectors, as well as identify policy issues that affect response and recovery.

The process incorporates existing entities across the public and private sectors, including the Government and Industry Sector Coordinating Councils, the US-CERT, the Homeland Security Information Network (HSIN), and Information Sharing and Analysis Centers (ISAC). It also builds on established Departmental practices and procedures for the identification, validation, coordination, and communication of vulnerabilities across the critical infrastructure sectors.

As part of this process, DHS relies on three primary mechanisms to communicate vulnerability information about control systems to the various stakeholders. The US-CERT National Cyber Alert System is utilized as a mechanism to share information about vulnerabilities to a broader audience. Vulnerability information is conveyed via several products, including *Vulnerability Notes* that are released on a regular basis to stakeholders in the control systems community. More detailed analyses of cyber vulnerabilities that may impact control systems are published via the *Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems*, whose recipients include governments and members of the control systems community. Both of these reports are posted on the US-CERT Control Systems Portal and are available to all portal members with access to the control systems section of the website, which encompasses representatives from the Federal, State, and local governments, Sector Specific Agencies, and control systems owners, operators, and vendors.

In addition, DHS works with vendors, owners, and operators to perform vulnerability assessments of selected systems to identify cyber vulnerabilities based on emerging exploits and partners with industry to develop mitigation strategies. DHS also works with control systems vendors, owners, and operators to share sensitive information through the Protected Critical Infrastructure Information (PCII) program so that private sector vulnerability data may be appropriately safeguarded.

Finally, in Fiscal Year (FY) 2007, we began working with our Federal partners to identify baseline individual agency activities to serve as the foundation for developing a comprehensive control systems strategy that will encompass the public and private sectors, set a national vision to secure control systems, describe roles and responsibilities, and identify future requirements for resources and actions. The Department has developed a timeline to complete this action, building on work that has already been completed. In the first quarter of FY 2008, a draft of the Federal sector portion of the strategy will be released for review by government stakeholders. Working with sector representatives from the Partnership for Critical Infrastructure Security under the NIPP framework, we will then begin to develop a private sector component to integrate into the strategy. We intend to have a final comprehensive strategy ready for release in the first quarter of FY 2009.

Conclusion

Securing control systems is an important priority for DHS because they are unique elements of our critical infrastructure. They are deployed ubiquitously and perform such vital functions that their disruption could severely impact citizens' daily lives. DHS has developed a program that includes the development and dissemination of tools, products, and guidance to the controls systems community, established mechanisms to work with our partners in both the government and industry, and developed capabilities to prepare for and respond to incidents.

Ongoing education and training for the control systems community is imperative, as well as regular assessments of systems. We must continue to raise awareness of the threats to and vulnerabilities of control systems through our information sharing mechanisms and continue to incorporate security measures in control systems standards. The development, execution, and maintenance of a national control systems security strategy is essential to managing our current and future efforts. The work we have accomplished so far has deepened our understanding of the challenges that lay before us, and we continue to work to strengthen our national control systems preparedness and protection posture.

Thank you for your time today, and I am happy to answer any questions from the Subcommittee.